PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-102734
(43)Date of publication of application : 16.04.1996

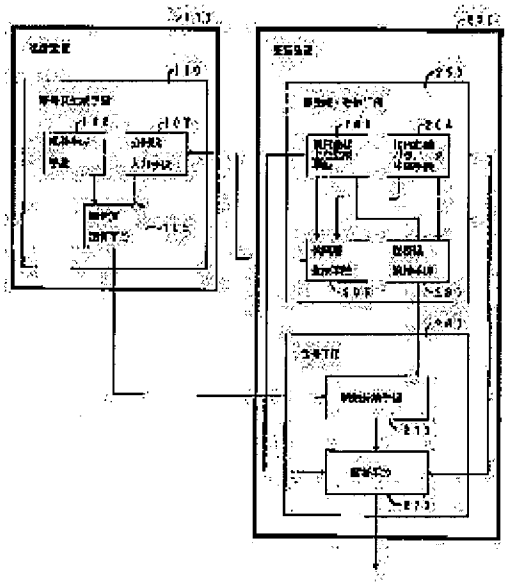
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G09C 1/00

(21)Application number : 06-236500
(22)Date of filing : 30.09.1994

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : OKAMOTO TATSUAKI

(54) PUBLIC KEY CRYPTOGRAPHIC METHOD/SYSTEM

(57)Abstract:
PURPOSE: To attain the ciphering by means of a single cryptogram by using the double cycle, i.e., the characteristic of an elliptical curve to use one of both cycles for the ciphering of a written message and the other cycle for the generation of random numbers in terms of probability respectively.
CONSTITUTION: In a public key cryptographic system that assures the communication secret between a transmission device 100 and a reception device 200, a public key is generated by means of an operation carried out on an elliptical curve. When a secret key is generated, a remainder operation and a weil pairing operation are carried out to the cryptogram received from the device 100 by means of a key generation/register means 250. Then a discrete logarithm problem is solved to the result of the weil pairing operation. Thus the cryptogram is restored into a normal message by a decoder means 260 of the device 200. In this respect the device 100 includes a cryptogram generation means 110. Then the means 250 includes a parameter generation means 204 which decides the parameters of a total number (n) and the elliptical curve, and a point generation means 203 which decides two points (G1, G2) on the elliptical curves En (a, b) in a remainder operation that defines a synthetic number (n) as the modulus.



LEGAL STATUS

[Date of request for examination] 14.10.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]	
[Date of final disposal for application]	
[Patent number]	3278790
[Date of registration]	22.02.2002
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－102734

(43)公開日　平成８年(1996)４月16日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		7259－5Ｊ		
				Ｈ０４Ｌ　9/ 00　Ｚ	

審査請求　未請求　請求項の数９　ＯＬ　（全 15 頁）

(21)出願番号　特願平6－236500

(22)出願日　平成６年(1994)９月30日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　岡本　龍明
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

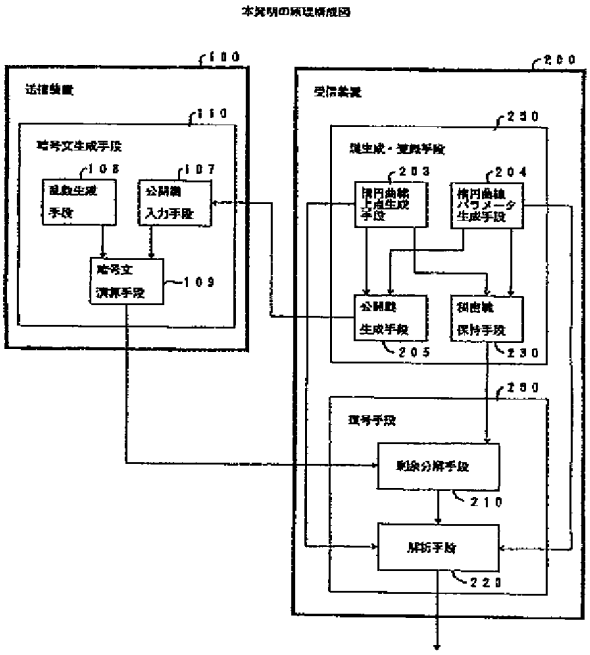
(74)代理人　弁理士　伊東　忠彦

(54)【発明の名称】　公開鍵暗号方法及び公開鍵暗号システム

(57)【要約】

【目的】　本発明の目的は、通信効率と復号処理効率が共に工場する公開鍵暗号方法及び公開鍵暗号システムを提供することである。

【構成】　本発明は、楕円曲線上の演算を利用して生成した公開鍵を公開し、秘密鍵を生成し、保持する鍵生成・登録手段２５０と、送信装置１００より受信した暗号文に対して剰余演算及びヴェイユ対演算を行い、ヴェイユ対演算の結果に対して離散対数問題を解くことにより暗号文を平文に復号する復号手段２６０とを有する受信装置２００と、受信装置２００から公開鍵を入手し、楕円曲線上の演算を利用して暗号文を生成する暗号文生成手段１１０を有する送信装置１００とを具備する。



1

【特許請求の範囲】

【請求項１】　送信装置と受信装置間の通信の秘密を保証する公開鍵暗号方法において、

該受信装置側では、

楕円曲線上の演算を利用して公開鍵及び秘密鍵を生成し、

生成された該公開鍵を公開し、

生成された該秘密鍵を保持し、

該送信装置側では、

該公開鍵を入手し、

該楕円曲線上の演算を利用して暗号文を生成して、該受信装置に送信し、

該受信側装置において、

該送信装置より受信した該暗号文に対して剰余演算及びヴェイユ対演算を行い、該ヴェイユ対演算の結果に対して離散対数問題を解くことにより該暗号文を平文に復号することを特徴とする公開鍵暗号方法。

【請求項２】　前記受信装置において、前記公開鍵及び前記秘密鍵を生成する際に、

予め合成数ｎ及び前記楕円曲線のパラメータ（ａ，ｂ）を定め、

さらに、該合成数ｎを法とする剰余演算における楕円曲線E_n（ａ，ｂ）上の２点（G_1，G_2）を定め、ｋ，ｎ，ａ，ｂ，G_1，G_2を前記公開鍵とし、

該合成数ｎの素因数を前記秘密鍵とする請求項１記載の公開鍵暗号方法。

【請求項３】　前記送信装置において、前記暗号文を生成する際に、

乱数γを生成し、

該乱数γと入力される通信文ｍを用いて、前記楕円曲線E_n（ａ，ｂ）上の前記合成数ｎを法とする剰余演算における前記楕円曲線上の演算を行い、前記暗号文ｃ（但し、$c = mG_1 + \gamma G_2$）を生成する請求項１記載の公開鍵暗号方法。

【請求項４】　前記受信装置において、前記暗号文を復号する際に、

前記送信装置より受信した前記暗号文を前記合成数ｎの素因数を法とする剰余演算の要素に分解し、

分解された要素に対して、ヴェイユ対演算を行い、該ヴェイユ対演算の演算値に対して離散対数問題を解き、

該離散対数問題の解を中国人剰余定理により復号文を生成する請求項１記載の公開鍵暗号方法。

【請求項５】　送信装置と受信装置間の通信の秘密を保証する公開鍵暗号システムにおいて、

楕円曲線上の演算を利用して公開鍵を生成して、公開し、秘密鍵を生成し、保持する鍵生成・登録手段と、

該送信装置より受信した該暗号文に対して剰余演算及びヴェイユ対演算を行い、該ヴェイユ対演算の結果に対して離散対数問題を解くことにより該暗号文を平文に復号する復号手段とを有する受信装置と、

2

該受信装置から該公開鍵を入手し、該楕円曲線上の演算を利用して暗号文を生成する暗号文生成手段を有する送信装置とを具備することを特徴とする公開鍵暗号システム。

【請求項６】　前記鍵生成・登録手段は、

合成数ｎ及び楕円曲線のパラメータ（ａ，ｂ）を定める楕円曲線パラメータ生成手段と、

該合成数ｎを法とする剰余演算における該楕円曲線E_n（ａ，ｂ）上の２点（G_1，G_2）を定める楕円曲線上点生成手段と、

該楕円曲線パラメータ生成手段により生成された該パラメータ（ａ，ｂ）及び該楕円曲線上点生成手段により生成された該２点（G_1，G_2）を用いて公開鍵ｋ，ｎ，ａ，ｂ，G_1，G_2を生成する公開鍵生成手段と、

該合成数ｎの素因数を秘密鍵として格納する秘密鍵保持手段とを含む請求項５記載の公開鍵暗号システム。

【請求項７】　前記復号手段は、

該送信装置から送信された前記暗号文ｃを該合成数ｎの素因数を法とする剰余演算の要素に分解する剰余分解手段と、

該剰余分解手段により分解された各要素にヴェイユ対演算を用いて離散対数問題を解き、前記暗号文を復号する解析手段とを含む請求項５記載の公開鍵暗号システム。

【請求項８】　前記解析手段は、

前記離散対数問題の解を中国人剰余定理により１つの復号文に変換する手段を含む請求項７記載の公開鍵暗号システム。

【請求項９】　前記暗号文生成手段は、

前記受信装置より前記公開鍵（ｋ，ｎ，ａ，ｂ，G_1，G_2）を入力する公開鍵入力手段と、

乱数γを生成する乱数生成手段と、

該乱数生成手段により生成された該乱数γと入力される通信文ｍを用いて前記楕円曲線E_n（ａ，ｂ）上の演算を前記合成数ｎを法とする剰余演算を行い、該通信文ｍを暗号文ｃ（但し、$c = mG_1 + \gamma G_2$）に暗号化する暗号文演算手段を含む請求項５記載の公開鍵暗号システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、公開鍵暗号方法及び公開暗号鍵システムに係り、特に、電気通信システムにおいて通信の秘密を保証して通信を行う公開鍵暗号方式（池野、小山著「現代暗号理論」電子情報通信学会）を実現する公開暗号方法及び公開鍵暗号システムに関する。

【０００２】詳しくは、ディジタル化された文書を伝送する際に、楕円曲線に基づいて公開鍵暗号を用いて安全性を高めることが可能な公開解暗号方法及び公開鍵暗号システムに関する。

【０００３】

3

【従来の技術】従来の第１の公開鍵暗号を安全に実現する方法として、GoldwasserとMicaliにより確率暗号が導入されている(Goldwasser, Micali, "Probabilistic Encryption," SIAM J. Computing (1984))。

【０００４】この"Goldwasser とMicali" による方法は、１ビットの情報m（mは０か１）を

【０００５】

【数１】

$$C = \begin{cases} \gamma^2 \bmod N & \text{IF } m = 0 \\ a\gamma^2 \bmod N & \text{IF } m = 1 \end{cases}$$

（但し、N，ａは公開鍵、γは乱数）

【０００６】のように暗号化している。この時の暗号文は、公開鍵のサイズと同様（略５００ビット）となる。

【０００７】また、従来の第２の公開鍵暗号の方法として、Cohen (Cohen,Hischer,"A Robust and Verifiable Cryptographically Secure Election Sechme", ProceedingofFoundation of Computer Science, pp. 372-382(1985) の高次剰余の理論に基づいて、より通信効率の良い方式を提案している。この方法は、ｔビットの情報mを

$c = a^m \cdot \gamma^L \bmod N$

というように暗号化する（但し、ａ，Ｎ，Ｌ（Ｌのサイズはｔビット以上）は公開鍵、γは乱数）。この暗号文ｃを復号するためには、情報mをしらみ潰し的に探索して復号する。

【０００８】

【発明が解決しようとする課題】しかし、上記の従来の第１の方法は、１ビットを暗号化すると５００ビットの暗号文となり、通信効率が非常に悪いという問題がある。

【０００９】また、上記の従来の第２の方法は、高次剰余の理論に基づいて上記の従来の第１の方法の問題を解決しているが、現在既知となっている全ての方法を用いても情報mをしらみ潰し的に探索する以外に復号する方法がない。

【００１０】例えば、情報mが１０ビットである場合は、０～2^{10}－１の１０２４通りの全ての値を復号式に代入して満足するものを見つける必要がある。従って、現在のコンピュータの能力では、通常2^{40}以上になると、１日以上、2^{60}程度では、スーパーコンピュータを用いても何十年もかかる計算となる。従って、通常の利用環境で、数秒以内程度で復号するためには、せいぜい１０ビット程度が限度である。

【００１１】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、通信効率と復号処理効率が共に向上する公開鍵暗号方法及び公開鍵暗号システムを提供することを目的とする。

4

【００１２】

【課題を解決するための手段】図１は、本発明の原理を説明するためのフローチャートである。

【００１３】本発明の公開鍵暗号方法は、送信装置と受信装置間の通信の秘密を保証する公開鍵暗号方法において、受信装置側では、楕円曲線上の演算を利用して公開鍵及び秘密鍵を生成し（ステップ１）、生成された公開鍵を公開し（ステップ２）、生成された秘密鍵を保持し（ステップ３）、送信装置側では、公開鍵を入手し、楕円曲線上の演算を利用して暗号文を生成し（ステップ４）、受信装置に送信し（ステップ５）、受信側装置では、送信装置より受信した暗号文に対して剰余演算及びヴェイユ対演算を行い、ヴェイユ対演算の結果に対して離散対数問題を解くことにより暗号文を平文に復号する（ステップ６）。

【００１４】また、受信装置において、公開鍵及び秘密鍵を生成する際に（ステップ１）、予め合成数ｎ及び前記楕円曲線のパラメータ（ａ，ｂ）を定め、さらに、合成数ｎを法とする剰余演算における楕円曲線E_n（ａ，ｂ）上の２点（G_1，G_2）を定め、ｋ，ｎ，ａ，ｂ，G_1，G_2を公開鍵とし、合成数ｎの素因数を秘密鍵とする。

【００１５】また、送信装置において、暗号文を生成する際に（ステップ４）、乱数γを生成し、乱数γと入力される通信文mを用いて、楕円曲線E_n（ａ，ｂ）上の合成数ｎを法とする剰余演算における楕円曲線上の演算を行い、暗号文ｃ（但し、$c = mG_1 + \gamma mG_2$）を生成する。

【００１６】また、受信装置において、暗号文を復号する際に（ステップ６）、送信装置より受信した暗号文を合成数ｎの素因数を法とする剰余演算の要素に分解し、分解された要素に対して、ヴェイユ対演算を行い、ヴェイユ対演算の演算値に対して離散対数問題を解き、離散対数問題の解を中国人剰余定理により復号文を生成する。

【００１７】図２は、本発明の原理構成図である。

【００１８】本発明は、送信装置１００と受信装置２００間の通信の秘密を保証する公開鍵暗号システムにおいて、楕円曲線上の演算を利用して公開鍵を生成して公開し、秘密鍵を生成し、保持する鍵生成・登録手段２５０と、送信装置１００より受信した暗号文に対して剰余演算及びヴェイユ対演算を行い、ヴェイユ対演算の結果に対して離散対数問題を解くことにより暗号文を平文に復号する復号手段２６０とを有する受信装置２００と、受信装置２００から公開鍵を入手し、楕円曲線上の演算を利用して暗号文を生成する暗号文生成手段１１０を有する送信装置１００とを具備する。

【００１９】また、上記の鍵生成・登録手段２５０は、合成数ｎ及び楕円曲線のパラメータ（ａ，ｂ）を定める楕円曲線パラメータ生成手段２０４と、合成数ｎを法と

する剰余演算における楕円曲線E_n（a，b）上の２点（G_1，G_2）を定める楕円曲線上点生成手段２０３と、楕円曲線パラメータ生成手段２０４により生成されたパラメータ（a，b）及び楕円曲線上点生成手段２０３により生成された２点（G_1，G_2）を用いて公開鍵k，n，a，b，G_1，G_2を生成する公開鍵生成手段２０５と、合成数nの素因数を秘密鍵として格納する秘密鍵保持手段２３０とを含む。

【００２０】また、上記の復号手段２６０は、送信装置１００から送信された暗号文cを合成数nの素因数を法とする剰余演算の要素に分解する剰余分解手段２１０と、剰余分解手段２１０により分解された各要素にヴェイユ対演算を用いて離散対数問題を解き、暗号文を復号する解析手段２２０とを含む。

【００２１】また、上記の解析手段２２０は、離散対数問題の解を中国人剰余定理により１つの復号文に変換する手段を含む。

【００２２】また、上記の暗号文生成手段１１０は、受信装置２００より公開鍵（k，n，a，b，G_1，G_2）を入力する公開鍵入力手段１０７と、乱数γを生成する乱数生成手段１０８と、乱数生成手段１０８により生成された乱数γと入力される通信文mとを用いて楕円曲線E_n（a，b）上の演算を合成数nを法とする剰余演算を行い、通信文mを暗号文c（但し、$c=mG_1+\gamma G_2$）を生成する暗号文演算手段１０９を含む。

【００２３】

【作用】本発明は、楕円曲線の特性である２重周期を利用するものであり、１つの周期を通信文の暗号化に用い、もう一方の周期を確率的に乱数化するために用いる。このように楕円曲線の２重周期を利用することにより、１個の暗号文で暗号化できる通信文のサイズが通信文の暗号化に用いる周期により決定される。

【００２４】また、復号処理では、ヴェイユ対（岡本・桜井著「代数幾何学的アルゴリズム」、情報処理、情報処理学会、Ｖｏｌ．３４．Ｎｏ．２，２月号(1993)）を利用することにより、乱数成分を除去し、さらに、離散対数問題を求める手法により復号化された通信文を求めることができる。

【００２５】

【実施例】図３は、本発明のシステム構成を示す。同図において、送信装置１００と受信装置２００が通信回線等３００を介して接続されている。受信装置２００は、鍵生成・登録部２５０と、復号部２６０より構成される。鍵生成・登録部２５０は、素数p，qの合成数n及び楕円曲線のパラメータ（a，b）を設定し、剰余演算における楕円曲線E_n（a，b）上の２点（G_1，G_2）を設定し、合成数n、及びパラメータa，bを公開鍵とし、また、合成数nの素因数を秘密鍵として保持する。また、復号部２６０は、入力された暗号文cを合成数nの素因数を法とする剰余演算の要素に分解し、分解された各要素毎に、ヴェイユ演算を用いて離散対数問題の解として通信文mを計算する。

【００２６】最初に受信装置の鍵生成・登録部２５０について説明する。

【００２７】［受信装置：鍵生成・登録部］図４は、本発明の一実施例の受信装置の鍵生成・登録部の構成を示す。受信装置２００の鍵生成・登録部２５０は、素数生成器２０１、乗算器２０２、楕円曲線パラメータ生成器２０３、楕円曲線上点生成器２０４、剰余定理演算器２０５、位相計算器２０６、最小公倍数演算器２０７より構成される。

【００２８】素数生成器２０１は、素数p，qを生成し、乗算器２０２及び楕円曲線パラメータ生成器２０３及び楕円曲線上点生成器２０４に出力する。乗算器２０２は、素数p，qを乗算し、$n=pq$とする。楕円曲線パラメータ生成器２０３は、入力された素数p，qを係数a，bに対し、パラメータ（a_p，b_p），（a_q，b_q）を楕円曲線上点生成器２０４、剰余定理演算器２０５及び位相計算機２０６に出力する。楕円曲線上点生成器２０４は、楕円曲線パラメータ生成器２０３より出力されたパラメータ（a_p，b_p），（a_q，b_q）と素数生成器２０１より出力された素数p，qにより、二重周期（G_{1p}，G_{2p}），（G_{1q}，G_{2q}）を取り出す。

【００２９】ここで、楕円曲線とは、素数pと係数a，bに対し、

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

を満たす点の集合に無限遠点Ｏを加えた集合

E_p（a，b）

にて定義される曲線をいう。

【００３０】次に、剰余定理演算器２０５は、中国人剰余定理により平文を求めるものであり、楕円曲線パラメータ生成器２０３より出力されるパラメータ（a_p，b_p），（a_q，b_q）と楕円曲線上点生成器２０４から出力される二重周期（G_{1p}，G_{2p}），（G_{1q}，G_{2q}）を用いて中国人剰余定理に基づいてa，b，G_1，G_2を計算する。位相計算器２０６は、素数生成器２０１より出力された素数p，q、楕円曲線上点生成器２０４から出力された二重周期（G_{1p}，G_{2p}），（G_{1q}，G_{2q}）と、楕円曲線パラメータ生成器２０３より出力されたパラメータ（a_p，b_p），（a_q，b_q）を用いて、位数（N_p，N_q，M_p，M_q）を求める。求められた位数は、最小公倍数演算器２０７に入力し、位数N_p，N_qについて最小公倍数を計算し、その結果ＬＣＭ（N_p，N_q）を合成数nの素因数とし、秘密鍵として格納する。

【００３１】図５は、本発明の一実施例の鍵生成・登録部の動作を説明するためのフローチャートである。

【００３２】ステップ１０１）素数生成器２０１は、素数p，qを生成する。

【００３３】ステップ１０２）乗算器２０２が、素数生

成器２０１より入力された素数ｐ，ｑを乗算し、合成数ｎを求める。

【００３４】ステップ１０３）楕円曲線パラメータ生成器２０３は、素数生成器２０１より素数ｐ，ｑが入力されると、楕円曲線のパラメータ（a_p，b_p），（a_q，b_q）を設定する。

【００３５】ステップ１０４）楕円曲線上点生成器２０４は、楕円曲線パラメータ生成器２０３より入力されたパラメータ（a_p，b_p），（a_q，b_q）と素数生成器２０１より入力された素数ｐ，ｑにより、剰余演算における楕円曲線E_n（ａ，ｂ）上の２点（二重周期（G_{1p}，G_{2p}），（G_{1q}，G_{2q}））を取り出す。

【００３６】ステップ１０５）次に、剰余定理演算器２０５は、楕円曲線パラメータ生成器２０３より入力されるパラメータ（a_p，b_p），（a_q，b_q）と楕円曲線上点生成器２０４から入力される二重周期（G_{1p}，G_{2p}），（G_{1q}，G_{2q}）を用いて中国人剰余定理に基づいて公開鍵（ａ，ｂ），（G_1，G_2）を計算する。

【００３７】ここで、公開鍵は、

$a \equiv a_p \pmod p$，

$a \equiv a_q \pmod q$，

$b \equiv b_p \pmod p$，

$b \equiv b_q \pmod q$，

$G_1 \equiv G_{1p} \pmod p$，

$G_1 \equiv G_{1q} \pmod q$，

$G_2 \equiv G_{2p} \pmod p$，

$G_2 \equiv G_{2q} \pmod q$

であるとする。

【００３８】ステップ１０６）位数計算器２０６は、素数生成器２０１より入力された素数ｐ，ｑ、楕円曲線上点生成器２０４から入力された二重周期（G_{1p}，G_{2p}），（G_{1q}，G_{2q}）と、楕円曲線パラメータ生成器２０３より入力されたパラメータ（a_p，b_p），（a_q，b_q）を用いて、以下の位数を求める。

【００３９】$N_p = ord_p\ (G_{1p})$

$N_q = ord_q\ (G_{1q})$

$M_p = ord_p\ (G_{2p})$

$M_q = ord_q\ (G_{2q})$

上記の位数N_pは、M_pの約数であり、N_qは、M_qの約数である。

【００４０】ステップ１０７）最小公倍数演算器２０７は、ステップ１０６により求められた位数N_p，N_qにより最小公倍数ＬＣＭ（N_p，N_q）を計算する。ここで、ｋ＋１を最小公倍数（ＬＣＭ（N_p，N_q））のビットサイズとする。

【００４１】ステップ１０８）上記の素数ｐ，ｑを秘密鍵として保持し、合成数ｎ、パラメータ（ａ，ｂ）、楕円曲線上の２点（G_1，G_2）及び最小公倍数のビットサイズｋを公開鍵とする。即ち、｛ｋ，ｎ，ａ，ｂ，G_1，G_2｝を公開鍵として公開する。

【００４２】次に、送信装置１００について説明する。

【００４３】［送信装置］図６は、本発明の一実施例の送信装置の構成を示す。送信装置１００は、乱数γを生成する乱数発生器１０８からの乱数γと、楕円曲線上の剰余演算を用いて受信装置２００に送信したい通信文ｍを暗号化し、暗号文ｃを出力する楕円曲線演算器１０９より構成される。

【００４４】楕円曲線演算器１０９は、受信装置２００から入力された公開鍵（ｎ，ａ，ｂ，G_1，G_2）、乱数発生器１０８から入力された乱数γ及び通信文ｍを用いて、

$c = mG_1 + \gamma G_2 \quad over \quad E_n\ (a, b)$

により暗号文ｃを求める。ここで、“＋”は、合成数ｎを法とする剰余演算における楕円曲線上の演算を意味し、mG_1は、$G_1 + G_1 + \cdots G_1$（ｍ回）を意味する。楕円曲線上の演算“＋”は、ｎを法とする剰余四則演算を繰り返し用いることにより実現できる（具体的には、以下の書籍等を参照されたい。N.Koblitz,"A cousrse in number theory and cryptography," GTM-114, Springer-Verlag,New York(1987)）。

【００４５】図７は、本発明の一実施例の送信装置の動作を示すフローチャートである。

【００４６】ステップ２０１）送信装置１００の乱数発生器１０８は乱数γを発生させる。

【００４７】ステップ２０２）受信装置２００に送信したい平文の通信文ｍを入力する。

【００４８】ステップ２０３）受信装置２００で生成された公開鍵ｎ，ａ，ｂ，G_1，G_2を入力する。

【００４９】ステップ２０４）送信装置１００は、乱数γ、通信文ｍ、公開鍵ｎ，ａ，ｂ，G_1，G_2を用いて、楕円曲線E_n（ａ，ｂ，）上の剰余演算をｍ回繰り返す。詳しくは、乱数γと公開鍵G_2を合成して、γG_2を生成し、通信文ｍと公開鍵G_1を合成してmG_1を生成する。次に、γG_2とmG_1を合成して暗号文ｃを生成する。

【００５０】ステップ２０５）送信装置１００は、暗号文ｃを出力する。

【００５１】次に、受信装置２００の復号部２６０について説明する。

【００５２】［受信装置：復号部］図８は、本発明の一実施例の受信装置の復号部の構成を示す。同図に示す受信装置２００の復号部２６０は、剰余演算器２１０、ヴェイユ対演算器２１１Ａ，Ｂ、離散対数演算器２１２、及び剰余定理演算器２０５を有する。このうち、同図においてヴェイユ対演算器２１１Ａ，２１１Ｂの２つが含まれているが、これは、１つの演算器として構成されてもよい。同図では、入出力が２種類あるために区別している。また、剰余定理演算器２０５は、鍵生成・登録部２５０の剰余定理演算器２０５と同様であり、一連の説明のために復号部２６０内に設けてあるものである。

【００５３】剰余演算器２１０は、送信装置１００から送信された暗号文ｃが入力されると、合成数ｎの素因数を法とする剰余演算の要素c_p，c_qに分解する。この要素c_p，c_qをヴェイユ対演算器２１１Ａに入力する。さらに、楕円曲線上の点G_{1p}，G_{1q}，G_{2p}，G_{2q}をヴェイユ対演算器２１１Ｂに入力する。これによりヴェイユ対演算器２１１Ａ，２１１Ｂはヴェイユ対演算を行い、演算結果を離散対数演算器２１２に入力する。離散対数演算器２１２は、鍵生成・登録部２５０の位数計算器２０６から位数N_p，N_qが入力され、離散対数の問題の解として復号された通信文ｍ（平文）が出力される。

【００５４】図９は、本発明の一実施例の受信装置の復号部の動作を示すフローチャートである。

【００５５】ステップ３０１）受信装置２００の剰余演算器２１０は、送信装置１００から暗号文ｃと素数ｐ，ｑの入力により、以下の剰余演算を行う。

【００５６】$c_p = c \bmod p$，
$c_q = c \bmod q$
を計算する。

【００５７】ステップ３０２）ステップ３０１で求めた剰余演算結果c_p、c_qと位数計算器２０６からの出力の楕円曲線上の点の位数M_p，M_q及び鍵生成・登録部２５０の楕円曲線上点生成器２０４により生成された楕円曲線上の点（G_{2p}、G_{2q}）をヴェイユ対演算器２１１Ａに入力する。また、鍵生成・登録部２５０の楕円曲線上点生成器２０４により生成された楕円曲線上の点（G_{1p}，G_{1q}）、（G_{2p}，G_{2q}）及び楕円曲線上の点の位数M_p，M_qをヴェイユ対演算器２１１Ｂに入力する。

【００５８】ステップ３０３）ヴェイユ対演算器２２１Ａは、位数M_p，M_qと剰余演算器２１０の出力c_p、c_q及び楕円曲線上の点（G_{2p}、G_{2q}）を用いて以下のヴェイユ対演算（ヴェイユ対演算の詳細は、岡本・桜井著「代数幾何学的アルゴリズム」情報処理学会誌、２月号（１９９３）を参照）を行う。

【００５９】$\beta_p = eM_p$（c_p，G_{2p}）
$\beta_q = eM_q$（c_q，G_{2q}）
これにより、第１のヴェイユ対β_p及びβ_qを求める。

【００６０】さらに、ヴェイユ対演算器２２１Ｂは、入力された楕円曲線上の点（G_{1p}，G_{1q}）、（G_{2p}，G_{2q}）及び楕円曲線上の点の位数M_p，M_qを用いて、以下により第２のヴェイユ対α_p，α_qを求める。

【００６１】$\alpha_p = eM_p$（G_{1p}，G_{2p}）
$\alpha_q = eM_q$（G_{1q}，G_{2q}）
ステップ３０４）次に、ヴェイユ対演算器２２１Ａ，２２１Ｂの演算結果β_p、β_q、α_p、α_q、最小公倍数N_p，N_q、素数ｐ，ｑを離散対数演算器２１２に入力する。

【００６２】ステップ３０５）離散対数演算器２１２は、入力されたβ_p、β_q、α_p、α_q、最小公倍数N_p，N_q、素数ｐ，ｑを用いて、以下の式を満足する離散対数の解m_p，m_qを求める。

【００６３】$\beta_p = \alpha_p^{m_p} \bmod p$
$\beta_q = \alpha_q^{m_q} \bmod q$
なお、上記の最小公倍数N_p，N_qは上記の式から消えているが、α_p、α_pの位数がN_p，N_qという事実を用いてm_p，m_qを求めるための入力として必要である（詳細は、池野・小山著「離散対数問題のポーリック・ヘルマン・アルゴリズム」参照）。

【００６４】ステップ３０６）離散対数演算の解m_p，m_q及び素数ｐ，ｑを中国人剰余定理演算器２０５に入力する。

【００６５】ステップ３０７）中国人剰余定理演算器２０５は、素数を用いて中国人剰余定理により平文ｍを求める。

【００６６】
$m \equiv m_p \pmod{N_p}$，　　…①
$m = m_q \pmod{N_q}$　　…②
上記の①及び②を合成することにより、平文ｍを導出する。

【００６７】上記の実施例のように、従来とは全く異なる数学的手段である楕円曲線を用いて暗号化及び復号化を行うものである。例えば、合成数ｎを５００ビット程度であるとすると、暗号文ｃは１０００ビット程度となる。

【００６８】また、ビットサイズｋを例えば、１００ビット程度にすることが可能であるため、１００ビットの平文を１０００ビットの暗号文に変換することが可能である。従来は、１ビットの平文に対して５００ビットの暗号文となっていたため、通信効率は１／５００であったが、本発明によれば、１００／１０００＝１／１０に向上させることができる。

【００６９】

【発明の効果】上述のように、本発明によれば、パラメータを適当に選ぶことにより、適当な大きさのビットサイズｋに対してｋビットの通信文を１つの暗号文ｃに暗号化できる。

【００７０】また、復号化処理は、ヴェイユ対演算と離散対数演算が大部分を占めるが、ヴェイユ対演算は、文献（岡本・桜井著「代数幾何学的アルゴリズム」情報処理、情報処理学会、Vol.34,No.2,2 月号(1993)）で述べられているように、効率的に（ｋの多項式のオーダ）で計算できる。また、N_p及びN_qが小さな素因数のみを含むようにすれば、離散対数演算も効率的に（ｋの多項式のオーダで）計算できる。

【００７１】これにより、従来の方式に比べて、本発明は、通信効率と復号処理効率が共に向上する。

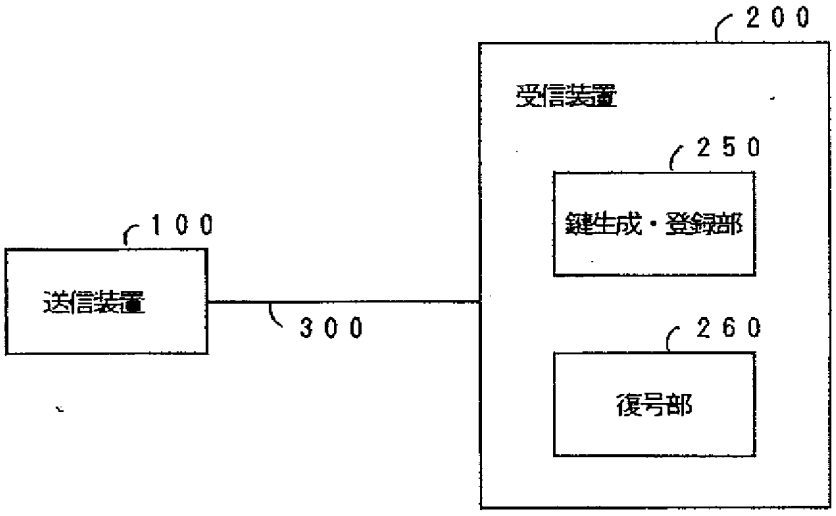
【図面の簡単な説明】

【図１】本発明の原理を説明するためのシーケンスチャートである。

【図２】本発明の原理構成図である。
【図３】本発明のシステム構成図である。
【図４】本発明の一実施例の公開暗号システムの受信装置の構成図である。
【図５】本発明の一実施例の鍵生成・登録部の動作を説明するためのフローチャートである。
【図６】本発明の一実施例の送信装置の構成図である。
【図７】本発明の一実施例の送信装置の動作を示すフローチャートである。
【図８】本発明の一実施例の受信装置の復号部の構成図である。
【図９】本発明の一実施例の受信装置の復号部の動作を示すフローチャートである。
【符号の説明】
１００　送信装置
１０７　公開鍵入力手段
１０８　乱数生成手段
１０９　暗号文演算手段
１１０　暗号文生成手段
２００　受信装置
２０１　素数生成器
２０２　乗算器
２０３　楕円曲線上点生成手段、楕円曲線パラメータ生成器
２０４　楕円曲線パラメータ生成手段、楕円曲線上点生成器
２０５　公開鍵生成手段、剰余定理演算器
２０６　位数計算器
２０７　最小公倍数演算器
２１０　剰余分解手段、剰余演算器
２１１　ヴェイユ対演算器
２１２　離散対数演算器
２２０　解析手段
２３０　秘密鍵保持手段
２５０　鍵生成・登録手段、鍵生成・登録部
２６０　復号手段・復号部

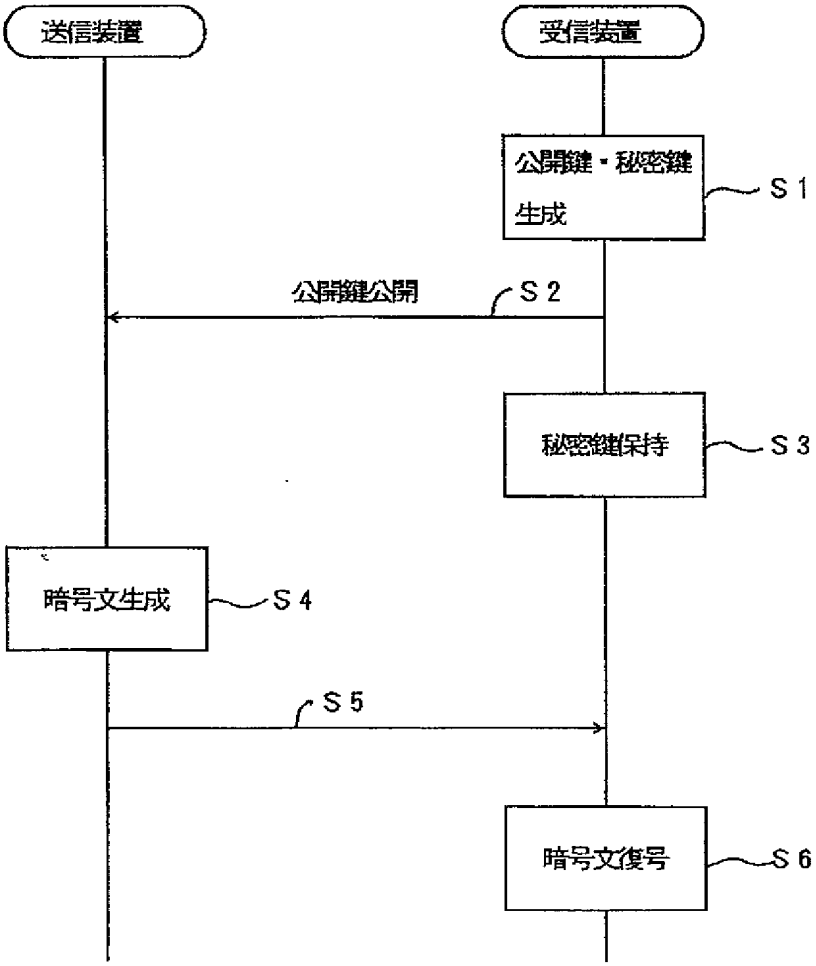
【図３】

本発明のシステム構成図



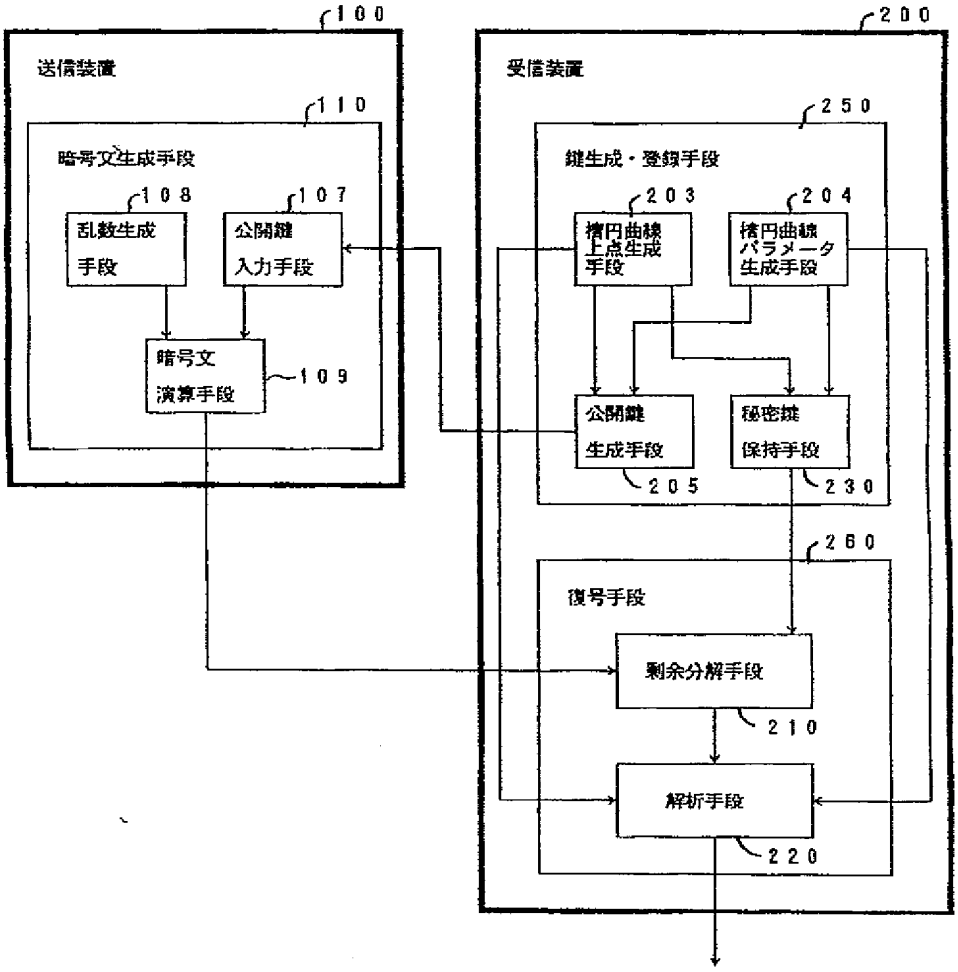
【図１】

本発明の原理を説明するためのフローチャート



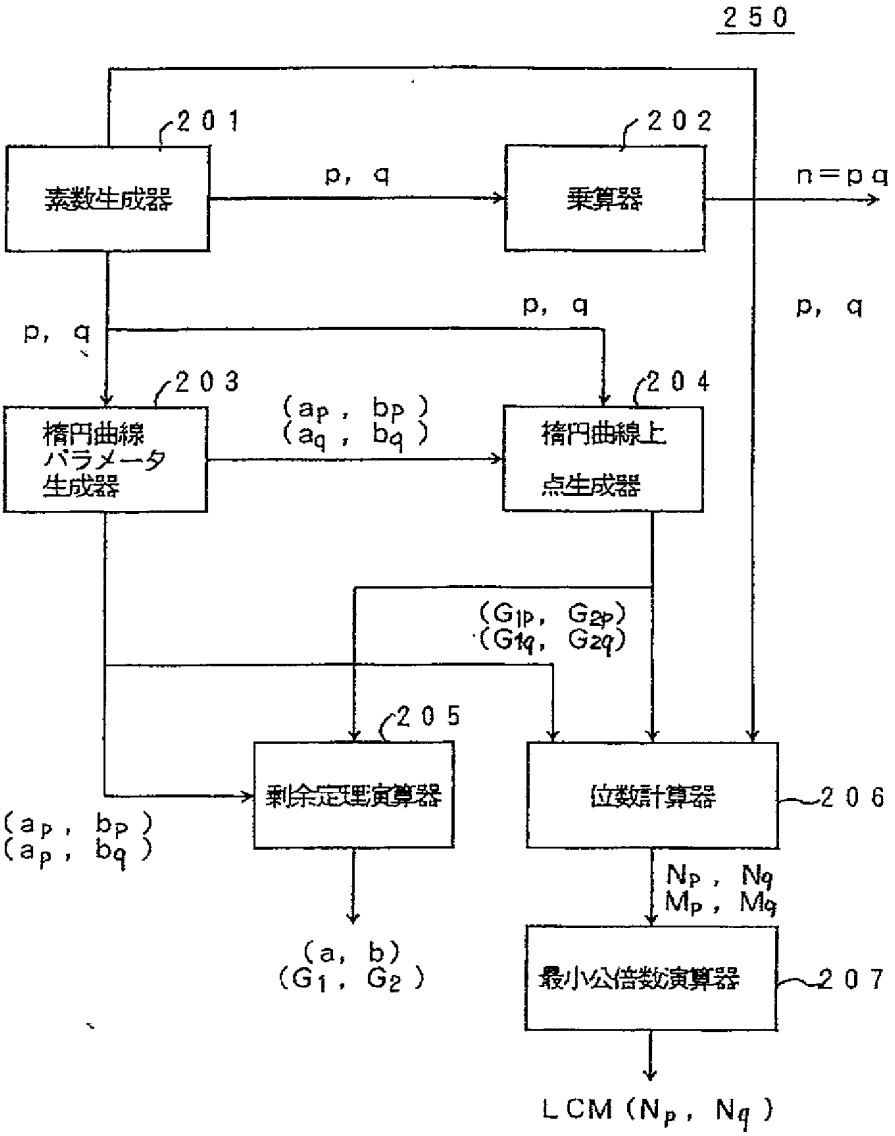
【図２】

本発明の原理構成図



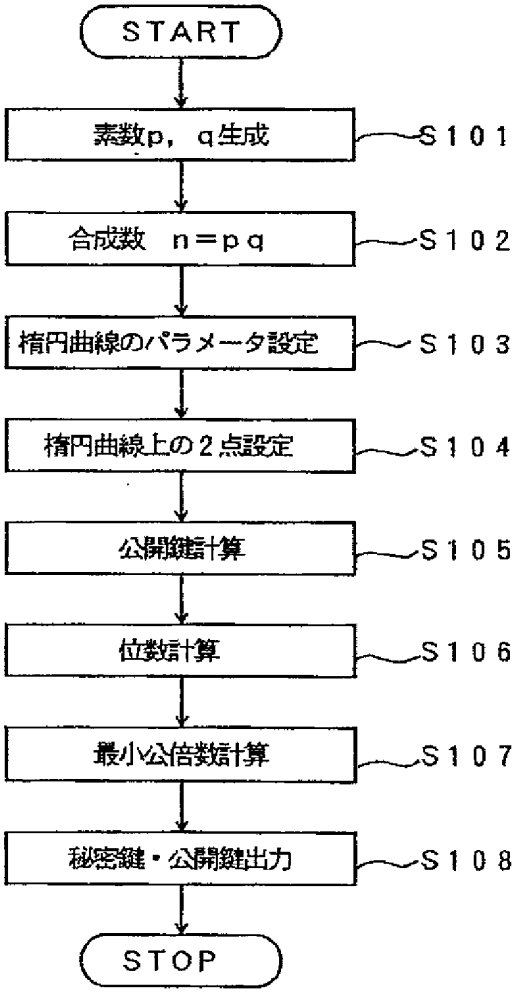
【図４】

本発明の一実施例の公開鍵暗号システムの受信装置の構成図



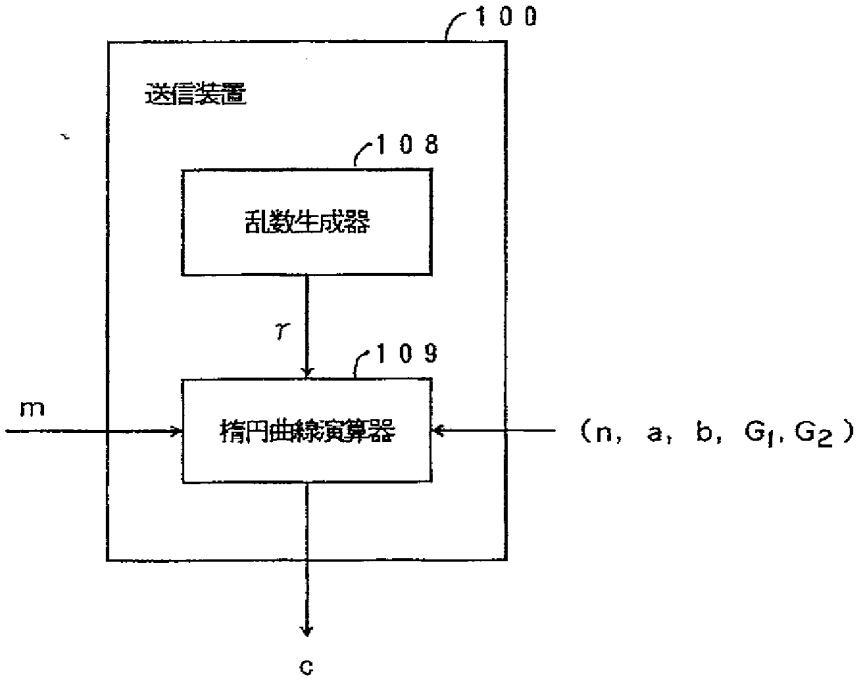
【図５】

本発明の一実施例の鍵生成・登録部の動作を説明するためのフローチャート



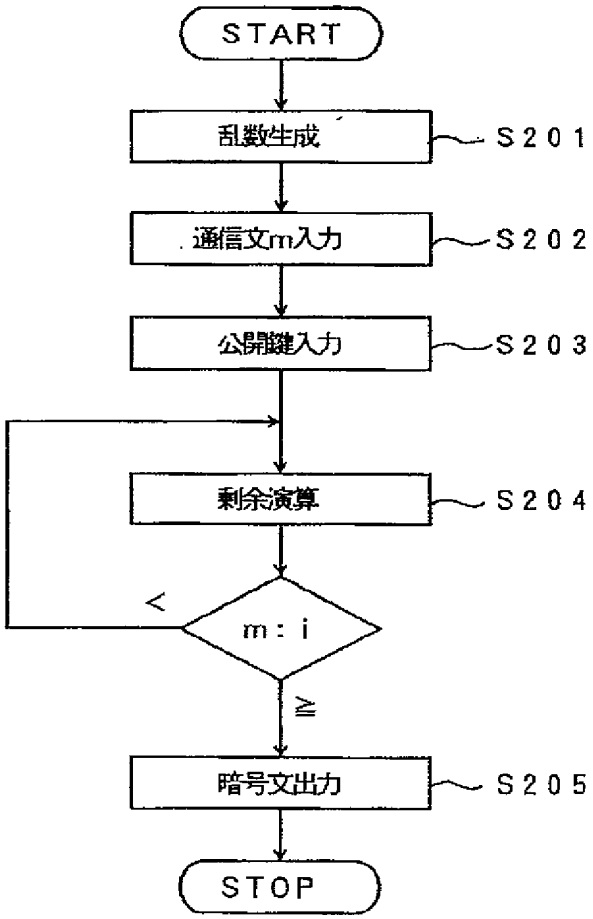
【図６】

本発明の一実施例の送信装置の構成図



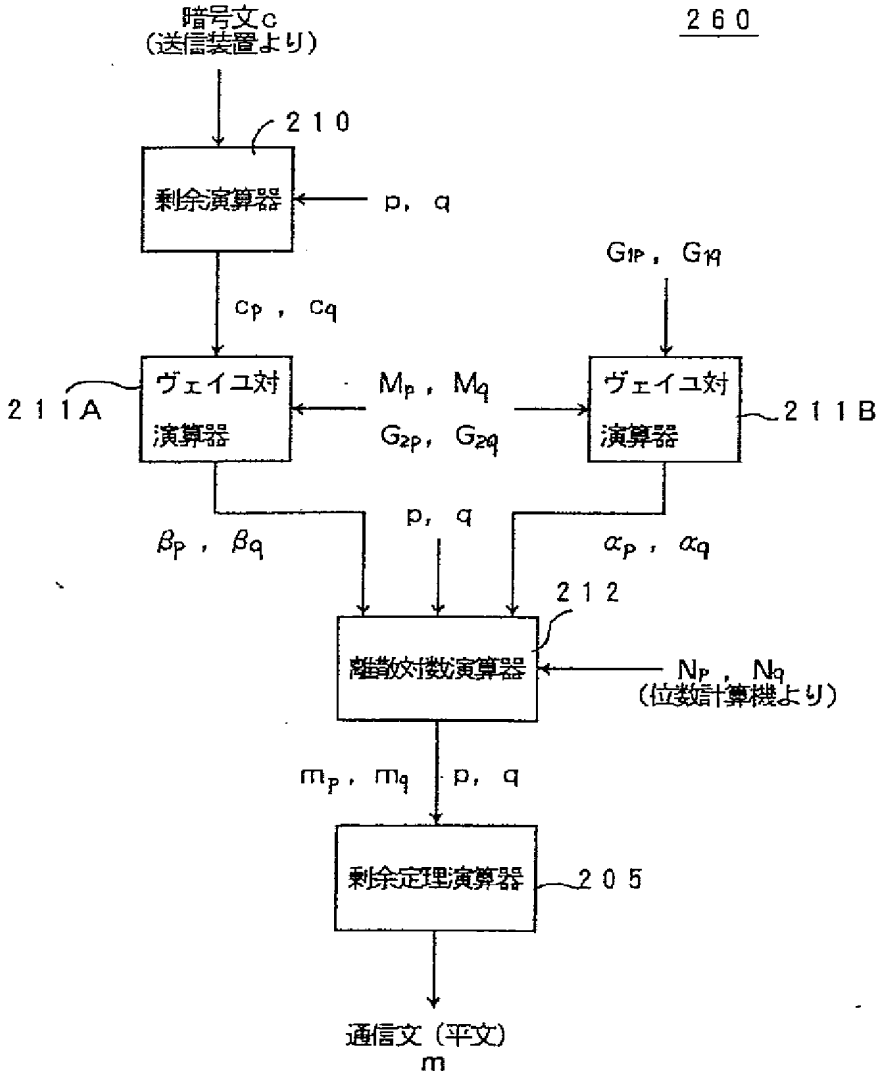
【図７】

本発明の一実施例の送信装置の動作を示すフローチャート



【図８】

本発明の一実施例の受信装置の復号部の構成図



【図９】

本発明の一実施例の受信装置の復号部の動作を示すフローチャート